Sweeping Changes Are in the Air for the HIPAA Security Rule

1/27/2025

Rule Proposal and Rationale

The U.S. Department of Health & Human Services, Office for Civil Rights (OCR) recently issued a Notice of Proposed Rulemaking (NPRM) to solicit comments on its proposal to overhaul and strengthen the HIPAA Security Rule and cybersecurity in the healthcare industry. If finalized, the proposed changes would significantly impact HIPAA covered entities, including healthcare providers, and their business associates. In its Fact Sheet, OCR emphasized that the "proposed rule seeks to strengthen cybersecurity by updating the Security Rule's standards to better address ever-increasing cybersecurity threats in the health care sector."

OCR indicated that the proposals are designed to address changes in the environment in which health care is provided, significant increases in breaches and cyberattacks, common deficiencies OCR has observed in investigations into Security Rule compliance, other cybersecurity guidelines, best practices, methodologies, procedures, and processes, and court decisions that affect enforcement of the Security Rule.

Proposed Revisions to Security Rule

Some of the proposed revisions include:

- Removing the distinction between "required" and "addressable" implementation specifications and making all implementation specifications required with specific, limited exceptions.
- Requiring written documentation of all Security Rule policies, procedures, plans, and analyses.
- Requiring the development and revision of a technology asset inventory and a network map that illustrates the movement of ePHI throughout the regulated entity's electronic information system(s) on an ongoing basis, but at least once every 12 months and in response to a change in the regulated entity's environment or operations that may affect ePHI.
- Requiring greater specificity for conducting a risk analysis.
- Strengthening requirements for planning for contingencies and responding to security incidents.
- Requiring regulated entities to conduct a compliance audit at least once every 12 months to ensure their compliance with the Security Rule requirements.
- Requiring that business associates verify at least once every 12 months for covered entities (and that business associate contractors verify at least once every 12 months for business associates) that they have deployed technical safeguards required by the Security Rule to protect ePHI through a written analysis of the business associate's relevant electronic information systems by a subject matter expert and a written certification that the analysis has been performed and is accurate.
- Requiring encryption of ePHI at rest and in transit, with limited exceptions.
- Requiring the use of multi-factor authentication, with limited exceptions.
- Requiring vulnerability scanning at least every six months and penetration testing at least once every 12 months.
- Requiring business associates to notify covered entities (and subcontractors to notify business associates) upon activation of their contingency plans without unreasonable delay, but no later than 24 hours after activation.

Written Comments to NPRM

Comments to the NPRM are due no later than March 7, 2025.

How We Can Help

If you have questions or would like assistance with your data privacy and security program, contact:

Lani M. Dornfeld, Esq., CHPC, *Member,* Healthcare Law at 973.403.3136 or ldornfeld@bracheichler.com

Authors

The following attorneys contributed to this insight.

Lani M. Dornfeld

CHPC, Member
Healthcare Law, Cannabis Industry

973.403.3136 · 973.618.5536 Fax

ldornfeld@bracheichler.com